WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Wednesday, March 22, 2006

Hide?	Set Name	Query	Hit Count
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L45	713/151,164,193;380/277,278;709/217,230.ccls. and (dynamic$7 near4 (tunnel or VPN) near4 config$7)and (higher or (lesser or lower))	0
☐	L44	713/151,164,193;380/277,278;709/217,230.ccls. and ISKMP and (security same higher same level$3)	0
☐	L43	713/151,164,193;380/277,278;709/217,230.ccls. and (ISKMP same security same higher same level$3)	0
☐	L42	L39 and Ipsec and (security$7 near3 config$7)	17
☐	L41	L39 and Ipsec and (security$7 near3 proposal$7)	3
☐	L40	L39 and Ipsec and (security$7 near proposal$7)	1
☐	L39	713/151,164,193;380/277,278;709/217,230.ccls. and (VPN)	301
	DB=PGPB; PLUR=YES; OP=OR		
☐	L38	L37 and higher adj level	4
☐	L37	((security adj (proposal$2 or polic$3)) near3 negotiat$4) and IPsec	29
☐	L36	(security adj (proposal$2 or polic$3)) near3 negotiat$4	36
☐	L35	L33 same (lower near2 security near2 level) and VPN	9
☐	L34	L33 same lower near2 security near2 level	77
☐	L32	(GREWAL near2 KARANVIR) and (VPN or tunnel)	1
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L31	GREWALnear2 KARANVIR and (VPN or tunnel)	1
☐	L30	GREWAL nrea2 KARANVIR and (VPN or tunnel)	872
☐	L29	L28 and IPsec	4
☐	L28	L27 same lower near2 level near2 security	151
☐	L27	higher near2 level near2 security	2207
☐	L26	automatic$4 near4 tunnel$6 near4 generat$7	31
☐	L25	L23 and (higher near2 (security or proposal$2))	2
☐	L24	L23 and ISAKMP	5
☐	L23	(dynamic$7 near4 (tunnel or VPN) near4 config$7)	43
☐	L22	(dynamic$7 near4 (tunnel or VPN) near4 config$7)and (higher or (lesser or lower))	18
☐	L21	(dynamic$7 near4 (tunnel or VPN) near4 congig$7)and (higher or (lesser or lower))	0
☐	L20	20020099668	2
☐	L19	security near5 proposal$4 same (tunnel or VPN)	8

☐	L16	(tunnel near5 config$6) same dynamic$7 and ISAKMP	1
☐	L15	(tunnel near5 config$6) same dynamic	25
☐	L14	L12 and (higher near5 level)	32
☐	L13	L12 same (higher near5 level)	0
☐	L12	ISAKMP same security	237
☐	L11	ISKMP	2
☐	L10	(ISKMP same security)	0
☐	L9	(ISKMP same security) and (higher same level)	0
☐	L8	ISKMP near5 security and (higher same level)	0
☐	L3	(726/15.ccls. and (security near2 proposal$7))	2
☐	L2	(bootable near3 windows and (program adj instructions or application) and device adj driver$5)	7
☐	L1	((ISAKMP and proposal$7) and (most near5 proposal$6))	5

END OF SEARCH HISTORY

STIC Search Report-3/22/2006

INVENTOR SEARCH - PATENTS

File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
(c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200618
(c) 2006 Thomson Derwent

Set	Items	Description
S1	6	AU=(GREWAL K? OR GREWAL, K?)
S2	34	AU=(GEORGESCU C? OR GEORGESCU, C?)
S3	1	S1 AND S2
S4	1	(S1 OR S2) AND (IPSEC OR VPN OR VIRTUAL()PRIVATE()NETWORK? ?)
S5	1	S3:S4

5/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015280324 **Image available**
WPI Acc No: 2003-341255/200332
XRPX Acc No: N03-272962
Tunnel configuration method for electronic communication, involves extracting security configuration from information transmitted by gateway to client, using which tunnel is established between client and gateway
Patent Assignee: INTEL CORP (ITLC); GEORGESCU C (GEOR-I); GREWAL K (GREW-I)
Inventor: **GEORGESCU C** ; **GREWAL K**
Number of Countries: 100 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030005328	A1	20030102	US 2001893736	A	20010629	200332 B
WO 200303689	A2	20030109	WO 2002US17134	A	20020530	200332
GB 2392805	A	20040310	WO 2002US17134	A	20020530	200418
			GB 200327185	A	20031121	
AU 2002259320	A1	20030303	AU 2002259320	A	20020530	200452
CN 1515107	A	20040721	CN 2002811599	A	20020530	200468
DE 10296987	T0	20041014	DE 10296987	A	20020530	200468
			WO 2002US17134	A	20020530	
GB 2392805	B	20050223	WO 2002US17134	A	20020530	200515
			GB 200327185	A	20020530	
AU 2002259320	A8	20051013	AU 2002259320	A	20020530	200611

Priority Applications (No Type Date): US 2001893736 A 20010629
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030005328	A1		12	H04L-009/00	
WO 200303689	A2	E		H04L-029/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN

IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

GB 2392805 A H04L-029/06 Based on patent WO 200303689
AU 2002259320 A1 H04L-029/00 Based on patent WO 200303689
CN 1515107 A H04L-029/06
DE 10296987 T0 H04L-029/00 Based on patent WO 200303689
GB 2392805 B H04L-029/06 Based on patent WO 200303689
AU 2002259320 A8 H04L-029/06 Based on patent WO 200303689

Abstract (Basic): US 20030005328 A1

NOVELTY - A negotiation is initiated by a client using a gateway which transmits information to the client. A security configuration is extracted by the client from the transmitted information, using which a tunnel is established between the client and the gateway.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) tunnel configuration system; and

(2) recorded medium storing tunnel configuration program.

USE - For configuring **virtual private network (VPN)** tunnels between client and gateway for electronic communication.

ADVANTAGE - Negotiation is initiated successfully and securely, thereby providing dynamic tunnel configuration with enhanced reliability.

DESCRIPTION OF DRAWING(S) - The figure shows a flow diagram explaining the tunnel configuration method.

pp; 12 DwgNo 4/7

Title Terms: TUNNEL; CONFIGURATION; METHOD; ELECTRONIC; COMMUNICATE; EXTRACT; SECURE; CONFIGURATION; INFORMATION; TRANSMIT; GATEWAY; CLIENT; TUNNEL; ESTABLISH; CLIENT; GATEWAY

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00; H04L-029/00; H04L-029/06

File Segment: EPI

INVENTOR SEARCH – NPL

File 8:Ei Compendex(R) 1970-2006/Mar W2
(c) 2006 Elsevier Eng. Info. Inc.

File 23:CSA Technology Research Database 1963-2006/Mar
(c) 2006 CSA.

File 35:Dissertation Abs Online 1861-2006/Feb
(c) 2006 ProQuest Info&Learning

File 65:Inside Conferences 1993-2006/Mar 20
(c) 2006 BLDSC all rts. reserv.

File 2:INSPEC 1898-2006/Mar W2
(c) 2006 Institution of Electrical Engineers

File 94:JICST-EPlus 1985-2006/Dec W4
(c)2006 Japan Science and Tech Corp(JST)

File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 10
(c) 2006 The Gale Group
File 6:NTIS 1964-2006/Mar W1
(c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Feb W4
(c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
(c) 2006 Inst for Sci Info
File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
(c) 2006 The HW Wilson Co.
File 95:TEME-Technology & Management 1989-2006/Mar W2
(c) 2006 FIZ TECHNIK
File 20:Dialog Global Reporter 1997-2006/Mar 20
(c) 2006 Dialog
File 256:TecInfoSource 82-2006/Feb
(c) 2006 Info.Sources Inc

Set Items Description
S1 125 AU=(GREWAL K? OR GREWAL, K?)
S2 190 AU=(GEORGESCU C? OR GEORGESCU, C?)
S3 0 S1 AND S2
S4 0 (S1 OR S2) AND (IPSEC OR VPN OR VIRTUAL()PRIVATE()NETWORK?
?)
S5 7 (S1 OR S2) AND NETWORK???
S6 5 RD (unique items)
? logoff hold
20mar06 15:31:50 User259273 Session D345.5

6/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02245944 E.I. Monthly No: EIM8705-030350
Title: PERSONALIZED COMMUNICATIONS: CONCEPTS AND PROTOTYPING.
Author: Feustel, T. C.; **Grewal, K. S.** ; Ordun, M. R.
Corporate Source: Bell Communications Research, Morristown, NJ, USA
Conference Title: GLOBECOM'86, IEEE Global Telecommunications Conference: Communications Broadening Technology Horizons - Conference Record.
Conference Location: Houston, TX, USA Conference Date: 19861201
Sponsor: IEEE Communications Soc, New York, NY, USA; IEEE, Houston Section, Houston, TX, USA; IEEE, Galveston Bay Section, TX, USA
E.I. Conference No.: 09431
Source: Publ by IEEE, New York, NY, USA. Available from IEEE Service Cent (Cat n 86CH2298-9), Piscataway, NJ, USA p 627-631
Publication Year: 1986
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8705
Abstract: The authors explore how the capabilities of intelligent **networks** can be harnessed to provide user control over universal communications services independently of time, place, and medium. An important tool is the modular integrated communications environment (MICE) testbed. The authors focus on existing and planned MICE services,

emphasizing the role of the MICE testbed as a research prototype for implementation of universal communications services. A brief description of MICE implementation with emphasis on aspects that facilitate provisioning of such services is given. Experiences to date and future plans are described. 11 refs.
Descriptors: *DIGITAL COMMUNICATION SYSTEMS--*Control; TELEPHONE; ELECTRONIC MAIL
Identifiers: MODULAR INTEGRATED COMMUNICATIONS ENVIRONMENT (MICE); UNIVERSAL COMMUNICATION SERVICES; PERSONALIZED COMMUNICATIONS; MICE HARDWARE ARCHITECTURE; USER CONTROL
Classification Codes:
716 (Radar, Radio & TV Electronic Equipment); 718 (Telephone & Line Communications); 723 (Computer Software)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

6/5/2 (Item 1 from file: 65)
DIALOG(R)File 65:Inside Conferences

00790113 INSIDE CONFERENCE ITEM ID: CN007720968
A Comparison between Fuzzy Logic, Neural Networks **and Conventional Approaches to System Modeling and Identification**
Georgescu, C. ; Afshari, A.; Bornard, G.
CONFERENCE: EUFIT '93-1st European congress on fuzzy and intelligent technologies
EUFIT -EUROPEAN CONGRESS-, 1993; VOL 3 P: 1632-1640
Aachen, Verlag der Augustinus, 1993
ISBN: 3860731769
LANGUAGE: English DOCUMENT TYPE: Conference Papers
CONFERENCE SPONSOR: European Laboratory for Intelligent Techniques Engineering
CONFERENCE LOCATION: Aachen, Germany
CONFERENCE DATE: Sep 1993 (199309) (199309)

BRITISH LIBRARY ITEM LOCATION: 3824.600000
NOTE:
In 3 vols
DESCRIPTORS: EUFIT; fuzzy technologies; intelligent technologies; ELITE

BIBLIOGRAPHIC PATENTS

File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)

File 350:Derwent WPIX 1963-2006/UD,UM &UP=200618

Set	Items	Description
S1	2237	VPN OR VIRTUAL()PRIVATE()NETWORK? ?
S2	275	IPSEC OR (IP OR INTERNET()PROTOCOL()SECURITY OR IPSECURITY

S3 77128 TUNNEL? ? OR SECURE(3N)CONNECT???? OR SSL OR SECURE()SOCKET()LAYER
S4 1278 SECURITY(3N)(ASSOCIATION? ? OR PARAMETER? ? OR SETTING? ? OR CONFIGURATION? ? OR PROPOSAL? ? OR NEGOTIAT????)
S5 13 S4(3N)(SORT??? OR ORDER??? OR RANK???)
S6 31058 SECUR???(3N)(MORE OR MOST OR HIGH??? OR GREATER OR GREATEST OR INCREAS??? OR MAXIMIZ??? OR MAXIMIS??? OR MAXIMIZATION OR MAXIMISATION OR MAXIMUM)
S7 18102 SECUR???(3N)(LESS OR LESSEN OR LESSENED OR LESSENING OR LEAST OR LOW??? OR DECREAS??? OR MINIMIZ??? OR MINIMIS??? OR MINIMIZATION OR MINIMISATION OR MINIMAL OR MINIMUM)
S8 9 S5 NOT AD=20010629:20030629/PR
S9 8 S8 NOT AD=20030629:20060320/PR
S10 0 S1:S3 AND S4 AND S6 AND S7
S11 127 S1:S3 AND S4
S12 10 S11 AND (S6 OR S7)
S13 2 S12 NOT AD=20010629:20030629/PR
S14 2 S13 NOT AD=20030629:20060320/PR
S15 8264 SECUR???(3N)(LEVEL? ? OR TIER? ? OR AMOUNT? ? OR STRICT? OR DEGREE?)
S16 1 S15 AND S11
S17 42 S11 AND IC=G06F
S18 32 S17 NOT AD=20030629:20060320/PR
S19 16 S18 NOT AD=20010629:20030629/PR
S20 14 S19 NOT (S9 OR S14)
S21 113 S11 AND IC=H04L
S22 82 S21 NOT S17
S23 56 S22 NOT AD=20030629:20060320/PR
S24 13 S23 NOT AD=20010629:20030629/PR
S25 435 (S6 OR S7)(5N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S26 12 S6(7N)S7(7N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S27 12 S26 NOT (S9 OR S14 OR S20 OR S24)
S28 6 S25 AND (S1:S3 OR SECURE()LINK? ?)
S29 6 S28 NOT (S9 OR S14 OR S20 OR S24)
S30 127 (S6 OR S7) AND S4
S31 65 S30 AND IC=H04L
S32 10 S31 AND (S1:S3 OR SECURE()LINK? ?)
S33 8 S32 NOT (S9 OR S14 OR S20 OR S24 OR S29)
S34 0 S33 NOT AD=20010629:20030629/PR
S35 35 S31 NOT AD=20010629:20030629/PR
S36 20 S35 NOT AD=20030629:20060320/PR
S37 17 S36 NOT (S9 OR S14 OR S20 OR S24 OR S29)
? logoff hold
20mar06 17:03:00 User259273 Session D345.12

24/5/10 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014295708 **Image available**
WPI Acc No: 2002-116411/200216

XRPX Acc No: N02-086915
Security protocol implementing system for electronic services supported through Internet, establishes tunnel **through an access controlling intermediate system, by** setting **up nested** security **session**
Patent Assignee: HEWLETT-PACKARD CO (HEWP)
Inventor: WRAY M
Number of Countries: 002 Number of Patents: 003
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
GB 2357226 A 20010613 GB 9929030 A 19991208 200216 B
US 20010023482 A1 20010920 US 2000733475 A 20001207 200216
GB 2357226 B 20030716 GB 9929030 A 19991208 200355

Priority Applications (No Type Date): GB 9929030 A 19991208
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
GB 2357226 A 55 H04L-009/12
US 20010023482 A1 H04L-012/22
GB 2357226 B H04L-009/12

Abstract (Basic): GB 2357226 A
NOVELTY - A security entity sets up secure communication sessions with peer security entities for passing application messages from protocol data units (PDU). A **tunnel** is established through an access controlling intermediate system, by **setting** up a nested **security** session whose PDU is encapsulated by PDU of primary session. The encapsulated PDU is identified by its message type field.
USE - For implementing security protocol for electronic services supported through Internet.
ADVANTAGE - Provides simple support for tunneling through access controlling intermediate system.
DESCRIPTION OF DRAWING(S) - The figure depicts tunneling supported by nested sessions established by session layer security protocol entity.
pp; 55 DwgNo 12/16
Title Terms: SECURE; PROTOCOL; IMPLEMENT; SYSTEM; ELECTRONIC; SERVICE; SUPPORT; THROUGH; ESTABLISH; **TUNNEL** ; THROUGH; ACCESS; CONTROL; INTERMEDIATE; SYSTEM; SET; UP; NEST; SECURE; SESSION
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/12** ; **H04L-012/22**
International Patent Class (Additional): **H04L-009/00** ; **H04L-029/06**
File Segment: EPI

24/5/12 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013583722 **Image available**
WPI Acc No: 2001-067929/200108
XRPX Acc No: N01-051761
Security **policy** setting **method in virtual communication network, involves specifying setting range, and choosing communication conditions from security policy information memory table**
Patent Assignee: MATSUSHITA ELECTRIC WORKS LTD (MATW)
Number of Countries: 001 Number of Patents: 001

Patent Family:
Patent No Kind Date Applicat No Kind Date Week
JP 2000324104 A 20001124 JP 99129152 A 19990510 200108 B

Priority Applications (No Type Date): JP 99129152 A 19990510
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 2000324104 A 12 H04L-012/24

Abstract (Basic): JP 2000324104 A
NOVELTY - The objective communication terminal devices are chosen on the screen on which a network map is displayed, and a setting range is specified. The communication conditions which should be set up are chosen from a security policy information memory table, in which communication conditions containing an encryption algorithm are stored beforehand.
DETAILED DESCRIPTION - A required communication path is searched on a network and the network apparatus that comprises each searched communication path is searched further in response to the selected setting range and selected communication conditions. The chosen communication conditions are set up automatically sequentially to each network apparatus. INDEPENDENT CLAIMS are also included for the following:
(a) a security policy manager;
(b) and a virtual communication network system.
USE - For virtual communication network.
ADVANTAGE - Allows automatic **setting** of **security** policy since designation of communication conditions is not performed. Enables automatic assembly of **virtual private network** and **setting** of **security** policy since only by designating the setting range on network map displayed by screen and choosing the communication conditions.
DESCRIPTION OF DRAWING(S) - The figure is a flowchart which shows a basic operation of the **security** policy **setting** method.
pp; 12 DwgNo 1/7
Title Terms: SECURE; SET; METHOD; VIRTUAL; COMMUNICATE; NETWORK; SPECIFIED; SET; RANGE; CHOICE; COMMUNICATE; CONDITION; SECURE; INFORMATION; MEMORY; TABLE
Derwent Class: W01
International Patent Class (Main): **H04L-012/24**
International Patent Class (Additional): **H04L-009/14** ; **H04L-012/26** ; H04M-011/00
File Segment: EPI

27/5/11 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013337341 **Image available**
WPI Acc No: 2000-509280/200046
XRPX Acc No: N00-376898
Data security device in information processing system, manages flow of data opposing to file accompanying process with lower order security **than the file accompanying process with** higher order security
Patent Assignee: NEC CORP (NIDE)
Number of Countries: 001 Number of Patents: 001

Patent Family:
Patent No Kind Date Applicat No Kind Date Week
JP 2000194591 A 20000714 JP 98368184 A 19981224 200046 B

Priority Applications (No Type Date): JP 98368184 A 19981224
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 2000194591 A 6 G06F-012/00

Abstract (Basic): JP 2000194591 A
NOVELTY - The flow of data opposing to file accompanying the process with **security** of **lower order** than that of file accompanying process with **higher order security** is managed.
USE - For controlling flow of data to perform data security in information processing system.
ADVANTAGE - Manages data flow effectively by preserving security to process and security to file.
pp; 6 DwgNo 1/3
Title Terms: DATA; SECURE; DEVICE; INFORMATION; PROCESS; SYSTEM; MANAGE; FLOW; DATA; OPPOSED; FILE; ACCOMPANIED; PROCESS; LOWER; ORDER; SECURE; FILE; ACCOMPANIED; PROCESS; HIGH; ORDER; SECURE
Derwent Class: T01
International Patent Class (Main): G06F-012/00
File Segment: EPI

FULL TEXT PATENTS

File 348:EUROPEAN PATENTS 1978-2006/ 200611
(c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060316,UT=20060309
(c) 2006 WIPO/Univentio

Set Items Description
S1 5476 VPN OR VIRTUAL()PRIVATE()NETWORK? ?
S2 4214 IPSEC OR (IP OR INTERNET()PROTOCOL)()SECURITY OR IPSECURITY OR IKE OR INTERNET()KEY()EXCHANGE OR ISAKMP
S3 49414 TUNNEL? ? OR SECURE(3N)(CONNECT???? OR LINK? ?) OR SSL OR SECURE()SOCKET()LAYER
S4 4193 SECURITY(3N)(ASSOCIATION? ? OR PARAMETER? ? OR SETTING? ? OR CONFIGURATION? ? OR PROPOSAL? ? OR NEGOTIAT????)
S5 113 S4(3N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S6 40449 SECUR???(3N)(MORE OR MOST OR HIGH??? OR GREATER OR GREATEST OR INCREAS??? OR MAXIMIZ??? OR MAXIMIS??? OR MAXIMIZATION OR MAXIMISATION OR MAXIMUM)
S7 33 S1:S3(S)S5
S8 28 S7 NOT AD=20010629:20030629/PR

S9 24 S8 NOT AD=20030629:20060320/PR
S10 21 S9 AND IC=(H04L OR G06F)
S11 87 S1:S3(S)S4(S)S6
S12 43 S11(S)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S13 42 S12 NOT S10
S14 38 S13 AND IC=(G06F OR H04L)
S15 29 S14 NOT AD=20010629:20030629/PR
S16 22 S15 NOT AD=20030629:20060320/PR
S17 29225 SECUR???(3N)(LESS OR LESSEN OR LESSENED OR LESSENING OR LEAST OR LOW??? OR DECREAS??? OR MINIMIZ??? OR MINIMIS??? OR MINIMIZATION OR MINIMISATION OR MINIMAL OR MINIMUM)
S18 25 S4(5N)S6(5N)S17
S19 23 S18 NOT (S10 OR S16)
S20 10 S19 NOT AD=20010629:20030629/PR
S21 6 S20 NOT AD=20030629:20060320/PR
S22 15269 SECUR???(3N)(LEVEL? ? OR TIER? ? OR AMOUNT? ? OR STRICT? OR DEGREE?)
S23 307 S22(10N)S4
S24 23 S23(S)S1:S3
S25 17 S24 NOT (S10 OR S16 OR S21)
S26 13 S25 NOT AD=20010629:20030629/PR
S27 9 S26 NOT AD=20030629:20060320/PR
S28 388 S4(5N)(S6 OR S17)
S29 50 S28(S)S1:S3
S30 45 S29 AND IC=(G06F OR H04L)
S31 29 S30 NOT AD=20010629:20030629/PR
S32 25 S31 NOT AD=20030629:20060320/PR
S33 14 S32 NOT (S10 OR S16 OR S21 OR S27)
S34 51 S1:S3(S)S4(S)S17
S35 25 S34 NOT (S10 OR S16 OR S21 OR S27 OR S33)
S36 11 S35 NOT AD=20010629:20030629/PR
S37 4 S36 NOT AD=20030629:20060320/PR
? logoff hold
21mar06 14:34:23 User259273 Session D347.6

10/3,K/12 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00858395 **Image available**
IPSEC PROCESSING
TRAITEMENT DU PROTOCOLE IPSEC
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGET LM ERICSSON (publ), S-126 25 Stockholm, SE, SE (Residence), SE (Nationality)
Inventor(s):
LINDBORG Seppo, Kuudestie 3, FIN-01510 Vantaa, FI,
TURTIAINEN Esa, Kartanonkuja 8 H, FIN-02360 Espoo, FI,
SCHULTZ Goran, Bjorkhagsgatan 10, FIN-21600 Pargas, FI,
KARNA Juha-Petri, Hakarinne 2 O 186, FIN-02100 Espoo, FI,
LINNAKANGAS Tommi, Piispantie 6 B 10, FIN-00370 Helsinki, FI,
Legal Representative:

GULLSTRAND Malin (agent), Ericsson Radio Systems AB, Patent Unit Research, S-164 80 Stockholm, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200191413 A2-A3 20011129 (WO 0191413)
Application: WO 2001SE960 20010503 (PCT/WO SE0100960)
Priority Application: GB 200012475 20000524
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 3651

Main International Patent Class (v7): **H04L-029/06**
Fulltext Availability:
Claims

English Abstract
A network device for implementing **IPSec** and comprising at least one IP forwarder (IPFW) arranged to receive IP packets each of...

...to implement security procedures for received IP packets in parallel. A security controller (SC) is **arranged** to allocate **negotiated** SAs amongst the **security** procedure modules and to notify the security procedure modules and the IP forwarder(s) of...

Claim
... arranged to implement security procedures for received IP packets in parallel; and a security controller **arranged** to allocate **negotiated** SAs amongst the **security** procedure modules and to notify the security procedure modules and the IP forwarder(s) of...

21/3,K/4 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00754060 **Image available**
AN APPARATUS FOR PROVIDING SECURE TRANSMISSION FOR FACSIMILE DATA MODEM SIGNALS
APPAREIL ASSURANT UNE TRANSMISSION SECURISEE DE SIGNAUX DE FAC-SIMILE SUR DES MODEMS DE DONNEES
Patent Applicant/Assignee:
AMIK INC, 10580 S.W. McDonald Street, Suite 202, Tigard, OR 97224, US, US (Residence), US (Nationality)
Inventor(s):

COLLETT Gordon C, 2155 N.W. Chrystal Drive, McMinnville, OR 97128, US
GALE Gary A, 47665 N.W. Deer Court, Box 5018, Manning, OR 97125, US
Legal Representative:
ROSENBERG Gerald B, 285 Hamilton Avenue, Suite 520, Palo Alto, CA 94301, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200067467 A1 20001109 (WO 0067467)
Application: WO 2000US11729 20000428 (PCT/WO US0011729)
Priority Application: US 99303203 19990430
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU CA IN MX
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 9303

Fulltext Availability:
Detailed Description

Detailed Description
... the passive pass-through mode; (2) whether the device is required to operate in a **low - security** mode, may attempt to **negotiate** a **high - security** mode, or may operate in the clear or any available **security** mode; (3) a **low - security** encoding key; and (4) a high-security key seed value. In alternate embodiments of the...

27/3,K/2 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00961954 **Image available**
A METHOD, SYSTEM, AND APPARATUS FOR PROVIDING SERVICES IN A PRIVACY ENABLED MOBILE AND UBICOM ENVIRONMENT
PROCEDE, SYSTEME ET APPAREIL PERMETTANT DE FOURNIR DES SERVICES DANS UN ENVIRONNEMENT MOBILE ET UBICOM A CONFIDENTIALITE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence), US (Nationality)
Inventor(s):
NORDMAN Ian, Opintie 2B 6, FIN-01150 Soderkulla, FI,
ALAMAKI Tero, Vanhaistentie 4D25, FIN-00420 Helsinki, FI,
VANSKA Marko, Nuolihaukantie 16A, FIN-02620 Espoo, FI,
TARKIAINEN Mikko, Iirislahdenportti 10D, FIN-02230 Espoo, FI,
GYORBIRO Norbert, Puistokaari 7A4, FIN-00200 Helsinki, FI,
GRIPENBERG Casper, Puistokaari 10A 11, FIN-00200 Helsinki, FI,
Legal Representative:
WASZKIEWICZ Kenneth (agent), c/o Morgan & Finnegan, LLP, 345 Park Avenue, New York, NY 10154-0053, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200296135 A1 20021128 (WO 0296135)
Application: WO 2002IB1697 20020517 (PCT/WO IB0201697)
Priority Application: US 2001860551 20010521
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 6209

Fulltext Availability:
Detailed Description

Detailed Description
... for user 100, controlling which types of services will receive profile data from user 100, **negotiating** the session **level security** such as **secure socket layer** (" **SSL** "), and providing a digital certificate to the terminal.

Session management 220 programs manage the communication...8 user 100 during communications with service operator 150. The parameters that Bluetooth device 110 **negotiates** include.

Security Level - Whether Bluetooth encryption is enabled and whether the
communication can utilize the **secure socket layer** ;
9 Privacy Level - Whether user 100 has preset the anonymity level;
Profile Access Level - Whether...with the ability to set and modify any property of the UTF. These properties include **negotiating** the session **level security** such as **secure socket layer** ("SSU), and providing a digital certificate to the ten-ninal.

9
Session management 264 programs...of user 100 during communications with Bluetooth device 110. The parameters that service operator 150 **negotiates** include.
Security Level - Whether Bluetooth encryption is enabled and whether the
communication can utilize the **secure socket layer** ;
9 Privacy Level - Whether user 100 has preset the anonymity level;
Profile Access Level - Whether...

33/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01211840

METHOD AND SYSTEM FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION WITH NETWORK SECURITY FEATURES

VERFAHREN UND SYSTEM ZUR NETZWERKADRESSUBERSETZUNG MIT SICHERHEITSEIGENSCHAFTEN

PROCEDE ET SYSTEME DESTINES A LA TRADUCTION REPARTIE D'ADRESSES RESEAU A L'AIDE DE DISPOSITIFS DE SECURITE DE RESEAU

PATENT ASSIGNEE:
3Com Corporation, (2692280), 3800 Golf Road, Rolling Meadows, IL 60008, (US), (Proprietor designated states: all)
INVENTOR:
GRABELSKY, David, A., 3800 Lee Street, Skokie, IL 60076, (US)
BORELLA, Michael, S., 1208 Haverhill Circle, Naperville, IL 60563, (US)
SIDHU, Ikhlaq, S., 403 East River Grove Lane, Vernon Hills, IL 60061, (US)
NESSETT, Danny, M., 34810 Wabash River Place, Fremont, CA 94555, (US)
LEGAL REPRESENTATIVE:
Gill, David Alan (69772), W.P. Thompson & Co., 55 Drury Lane, London WC2B 5SQ, (GB)

PATENT (CC, No, Kind, Date): EP 1159815 A1 011205 (Basic)
EP 1159815 B1 051123
WO 2000056034 000921
APPLICATION (CC, No, Date): EP 2000914989 000315; WO 2000US7057 000315
PRIORITY (CC, No, Date): US 270967 990317
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS (V7): **H04L-029/06** ; **H04L-029/12**
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS B (English) 200547 288
CLAIMS B (German) 200547 288
CLAIMS B (French) 200547 360
SPEC B (English) 200547 17786
Total word count - document A 0
Total word count - document B 18722
Total word count - documents A + B 18722

INTERNATIONAL PATENT CLASS (V7): **H04L-029/06** ...

... **H04L-029/12**

...SPECIFICATION Internet Protocol packet (e.g., to decrypt it, or to verify its integrity and authenticity).
Internet Protocol security establishes and uses a Security Association ("SA") to identify a secure channel between two endpoints...

...termination endpoints of a single Security Association define a logical session that is protected by **Internet Protocol security** services. One endpoint sends Internet Protocol packets, and a second endpoint receives the Internet Protocol packets. Since a **Security Association**

is unidirectional, a **minimum** of two **Security Associations** is required for secure, bi-directional communications. It is also possible to configure multiple layers of **Internet Protocol security** protocols between two endpoints by combining multiple Security Associations.

There are several problems associated with...

...Preferably said routing device is a distributed network address translation router.

Conveniently, said one or **more** locally unique **security** values are one or **more security parameter** indexes for an **Internet Protocol security** protocol.

Also, said Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated...

...CLAIMS distributed network address translation router.

3. The method of Claim 1 wherein the one or **more** locally unique **security** values are one or **more security parameter** indexes for an **Internet Protocol security** protocol.
4. The method of Claim 3 wherein the Internet Protocol security protocol is any...

33/3,K/6 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00924251 **Image available**
THIRD PARTY VPN CERTIFICATION
CERTIFICATION DE RESEAU VPN DE TIERS
Patent Applicant/Assignee:
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, 10260 Campus Point Drive, San Diego, CA 92121, US, US (Residence), US (Nationality)
Inventor(s):
LARSON Victor, 12026 Lisa Marie Court, Fairfax, VA 22033, US,
Legal Representative:
WRIGHT Bradley C (agent), Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, D.C. 20001-4597, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200258339 A1 20020725 (WO 0258339)
Application: WO 2002US1070 20020117 (PCT/WO US0201070)
Priority Application: US 2001262036 20010118; US 2001874258 20010606
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 10105

Main International Patent Class (v7): **H04L-012/50**
Fulltext Availability:
Detailed Description

Detailed Description
... that is registered with a central certificate server (repository).

The wildcard flag for specifying a **VPN** name pair can be extended to a wildcard that includes all names in which **VPN** 's of opportunity are automatically established with all **VPN** devices that are registered with the central certificate server. For example, when the **VPN** device 400 receives an scom request for establishing a **VPN** to another site, **VPN** device 400 looks in VPNbyName table 403 for the local name that is to be used by **VPN** device 400 for representing **VPN** device 400 to the other site. For instance, when a user on the nodel.acme...

...acme.scom,
remote-name = *.acme.scom, then the connection rule would automatically allow an outbond **VPN** request to www.node1acme.scom. Accordingly, the **VPN** device at
www.node2.acme.scom, would also need a matching connection rule local-name...

...node2.acme.scom, remote-name = *.acme.scom contained within the VPNbyName table so that the **VPN** request would be accepted. The **VPN** device at www.node2.acme.scom would authenticate the inbound **VPN** request and respond
17
accordingly so that the **VPN** will be set up,
SecurityPolicy table 404 associates a local name (i.e., the scom name that is being used for representing the **VPN** device on the network) with a particular signed certificate. A host computer can have several...

...names that are each tied to a respectively different security policy, signed certificate and the **VPN** network parameters for one side of a **VPN** . Specifically, for each local name in SecurityPolicy table 404, SecurityPolicy table 404 contains information relating to the client network address block, the IP address of the **VPN** device, the gateway IP address, and the allowable range of **VPN** **security** **parameters** (including **minimum** and maximum acceptable encryption algorithms, key lengths, and rekey rates). Accordingly, the client network address...

33/3,K/11 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00784140
A SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR A GLOBALLY ADDRESSABLE INTERFACE IN A COMMUNICATION SERVICES PATTERNS ENVIRONMENT
SYSTEME, PROCEDE ET ARTICLE DE FABRICATION S'APPLIQUANT DANS UN ENVIRONNEMENT DE STRUCTURE DE SERVICES DE COMMUNICATIONS VIA UNE INTERFACE ADRESSABLE GLOBALEMENT
Patent Applicant/Assignee:

ACCENTURE LLP, 1661 Page Mill Road, Palo Alto, CA 94304, US, US
(Residence), US (Nationality)
Inventor(s):
BOWMAN-AMUAH Michel K, 6426 Peak Vista Circle, Colorado Springs, CO 80918
, US,
Legal Representative:
HICKMAN Paul L (agent), Oppenheimer Wolff & Donnelly, LLP, 1400 Page Mill
Road, Palo Alto, CA 94304, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200116735 A2-A3 20010308 (WO 0116735)
Application: WO 2000US24198 20000831 (PCT/WO US0024198)
Priority Application: US 99387214 19990831
Designated States:
(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)
AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CU CZ DE DK DZ EE ES FI GB
GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK
MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN
YU ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 150371

Main International Patent Class (v7): **G06F-009/46**
Fulltext Availability:
Detailed Description

Detailed Description
... may include global transaction coordination, distributed two-phase commit, database support, coordinated recovery after failures, **high** availability, **security** , and work load balancing. TP services may utilize Messaging services, which provide basic interprocess communication...forums, LDAP for directory access, HTTP and HTML for access via a web browser, and **SSL** for security.

The following products are examples of e-mail systems.

Microsoft Mail
Lotus cc...Stronghold; UkWeb's SafePassage
UkWeb's Stronghold
Stronghold was the first web server to support **SSL** Client Authentication. Regular expressionbased matching of client certificate information to determine access control is possible...

...hardware products.

Application layer - data is encrypted by the application. Netscape's Secure Sockets Layer (**SSL**) is one example of application-layer encryption for WWW browsers. **SSL** uses RSA encryption to wrap security information around TCP/IP based protocols.

Network layer - data...

...network layer header, therefore relying on the network layer protocol.
Implementation considerations
The advantage of **SSL** over S/HTTP is that **SSL** is not restricted to HTTP but can also be used for securing other TCP/IP based services such as FTP, Telnet, etc. **SSL** can provide session level data encryption and authentication to enable secure data communications over public...

...key issue in international e-commerce today.

Possible Product Options
Netscape's Secure Sockets Layer (**SSL**); S-HTTP; e-mail encryption; S-MIME
Encryption that is architected into Web-based solutions
Netscape's Secure Sockets Layer (**SSL**) - provides encryption for World Wide Web browsers.

S-HTTP - a secure version of the HTTP...network and an untrusted external network.)
The following IETF standard supports interoperability among security systems.

IPSec Allows two nodes to dynamically agree on a security association based on keys, encryption, authentication...
...before any communications take place; operates in the IP layer and supports TCP or UDP. **IPSec** will be included as part of IPng, or the next generation of 1P.

Implementation considerations...

...Networks; 3Com Corp.; Check Points Firewall-1; Raptor Systems Eagle Firewall; Data Fellows F-Secure **VPN** ; Racals Datacryptor 64F
The following are examples of vendors of products that perform Transport-level...

...s BorderWare Firewall Server
Raptor Systems' Eagle Firewall
encryption devices.

180
Data Fellows' F-Secure **VPN**
Racal's Datacryptor 64F
The following are examples of products that perform Transport-level
packet...connection release failure probability - fraction of release attempts which do not
succeed
protection - specifies a **secure connection**
priority - indicates traffic priority over the connection
resilience - probability that the transport layer spontaneously terminates...

33/3,K/14 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00742649 **Image available**
**METHOD AND SYSTEM FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION WITH NETWORK
SECURITY FEATURES**
**PROCEDE ET SYSTEME DESTINES A LA TRADUCTION REPARTIE D'ADRESSES RESEAU A
L'AIDE DE DISPOSITIFS DE SECURITE DE RESEAU**

Patent Applicant/Assignee:
3COM CORPORATION, 3800 Golf Road, Rolling Meadows, IL 60008, US, US (Residence), US (Nationality)
Inventor(s):
GRABELSKY David A, 3800 Lee Street, Skokie, IL 60076, US
BORELLA Michael S, 1208 Haverhill Circle, Naperville, IL 60563, US
SIDHU Ikhlaq S, 403 East River Grove Lane, Vernon Hills, IL 60061, US
NESSETT Danny M, 34810 Wabash River Place, Fremont, CA 94555, US
Legal Representative:
LESAVICH Stephen, McDonnell Boehnen Hulbert & Berghoff, 300 South Wacker Drive, Chicago, IL 60606, US

Patent and Priority Information (Country, Number, Date):
Patent: WO 200056034 A1 20000921 (WO 0056034)
Application: WO 2000US7057 20000315 (PCT/WO US0007057)
Priority Application: US 99270967 19990317
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CA DE GB JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 24220

Main International Patent Class (v7): **H04L-029/06**
International Patent Class (v7): **H04L-029/12**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... Internet Protocol packet (e.g., to decrypt it, or to verify-its integrity and authenticity).

Internet Protocol security establishes and uses a Security Association ("SA") identify a secure channel between two endpoints. A...

...terinination endpoints of a sinorle Security Association define a logical session that is protected by **Internet Protocol security** services. One endpoint sends Internet Protocol packets, and a second endpoint receives the Internet Protocol packets. Since a **Security Association** is unidirectional, a **minimum** of two **Security Associations** is required for secure, bidirectional communications. It is also possible to configure multiple layers of **Internet Protocol security** protocols between two endpoints by combining multiple Security Associations.

There are several problems associated with....

Claim
... distributed network address translation router.

4 The method of Claim I wherein the one or **more** locally unique **security**
values are one or **more security parameter** indexes for an **Internet Protocol security** protocol. 68 . The method of Claim 4 wherein the **Internet Protocol security** protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol or an **Internet Key Exchange** protocol.

6 The method of Claim I wherein the first protocol is a Port Allocation
...

...0 network address translation router.

12 The method of Claim 9 wherein the one or **more** locally unique **security**
values include one or **more security parameter** indexes for an **Internet Protocol**
Security Protocol
1 5

13 The method of Claim IO wherein the Internet Protocol security protocol
...

...list of one or more locally unique
security values is a list of one or **more security parameter** indexes for **Internet Protocol security** protocol.

17 The method of Claim 14 wherein the Internet Protocol security protocol is any...the method of Claim 28.

30 The method of Claim 28 wherein the one or **more** locally unique **security** values are **security parameter** indexes from an **Internet Protocol security** protocol.
3 1. The method of Claim 28 wherein the second network device is a... distributed network address translation router.

38 The system of Claim 36 wherein the one or **more** locally unique **security** values are one or **more security parameter** indexes for an **Internet Protocol security** protocol.
39 The system of Claim 36 wherein the secure virtual connection is an Internet...

****

BIBLIOGRAPHIC NPL

****

File 2:INSPEC 1898-2006/Mar W2
(c) 2006 Institution of Electrical Engineers
File 6:NTIS 1964-2006/Mar W2
(c) 2006 NTIS, Intl Cpyrght All Rights Res
File 8:Ei Compendex(R) 1970-2006/Mar W2
(c) 2006 Elsevier Eng. Info. Inc.
File 23:CSA Technology Research Database 1963-2006/Mar
(c) 2006 CSA.
File 34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
(c) 2006 Inst for Sci Info
File 35:Dissertation Abs Online 1861-2006/Feb
(c) 2006 ProQuest Info&Learning
File 65:Inside Conferences 1993-2006/Mar 21
(c) 2006 BLDSC all rts. reserv.
File 94:JICST-EPlus 1985-2006/Dec W4
(c)2006 Japan Science and Tech Corp(JST)
File 99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
(c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 13
(c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W4
(c) 2006 INIST/CNRS
File 239:Mathsci 1940-2006/Apr
(c) 2006 American Mathematical Society
File 256:TecInfoSource 82-2006/Feb
(c) 2006 Info.Sources Inc

Set Items Description
S1 8613 VPN OR VIRTUAL()PRIVATE()NETWORK? ?
S2 3582 IPSEC OR (IP OR INTERNET()PROTOCOL)()SECURITY OR IPSECURITY OR IKE OR INTERNET()KEY()EXCHANGE OR ISAKMP
S3 368107 TUNNEL? ? OR SECURE(3N)(CONNECT???? OR LINK? ?) OR SSL OR SECURE()SOCKET()LAYER
S4 3827 SECURITY(3N)(ASSOCIATION? ? OR PARAMETER? ? OR SETTING? ? OR CONFIGURATION? ? OR PROPOSAL? ? OR NEGOTIAT????)
S5 12 S4(3N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S6 29371 SECUR???(3N)(MORE OR MOST OR HIGH??? OR GREATER OR GREATEST OR INCREAS??? OR MAXIMIZ??? OR MAXIMIS??? OR MAXIMIZATION OR MAXIMISATION OR MAXIMUM)
S7 5738 SECUR???(3N)(LESS OR LESSEN OR LESSENED OR LESSENING OR LEAST OR LOW??? OR DECREAS??? OR MINIMIZ??? OR MINIMIS??? OR MINIMIZATION OR MINIMISATION OR MINIMAL OR MINIMUM)
S8 33 S1:S3 AND S4 AND (S6 OR S7)
S9 29 RD (unique items)
S10 13 S9 NOT PY=2002:2006
S11 3 S5 NOT PY=2002:2006
S12 10384 SECUR???(3N)(LEVEL? ? OR TIER? ? OR AMOUNT? ? OR STRICT? OR DEGREE?)
S13 8 S12 AND S4 AND S1:S3

S14 7 RD (unique items)
S15 3 S14 NOT PY=2002:2006
S16 547 (S6 OR S7)(3N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S17 11 S16 AND (S1:S3 OR S4)
S18 8 RD (unique items)
S19 165 S4(5N)(S6 OR S7)
S20 34 S4 AND S6 AND S7
S21 24 RD (unique items)
S22 17 S21 NOT PY=2002:2006
S23 17 S22 NOT (S11 OR S15 OR S18)
? logoff hold
21mar06 15:38:45 User259273 Session D347.12

10/5/4 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01690582 ORDER NO: AAD99-19204
TOWARDS NETWORK SECURITY MANAGEMENT IN AN INTERNETWORK ENVIRONMENT
Author: MAUGHAN, WILLIAM DOUGLAS
Degree: PH.D.
Year: 1998
Corporate Source/Institution: UNIVERSITY OF MARYLAND BALTIMORE COUNTY (0434)
Adviser: DEEPINDER P. SIDHU
Source: VOLUME 60/02-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 717. 229 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

The Internet has evolved into a critical communications infrastructure for commercial and private communications, both national and international. As the quantity of communications across computer networks grows, the need to **secure** these transmissions also **increases** .

The **security** required for communications depends on the specific network configuration and environment. Organizations are setting up **Virtual Private Networks** (VPNs) that require one set of security functions for communications within the **VPN** and, possibly, many different security functions for communications outside the **VPN** . These requirements allow the organization to support geographically separate components, customers, suppliers, sub-contractors (with their own VPNs), government, and other partners. Departments within large organizations may require security functionality to separate and protect data (e.g. personnel, company proprietary, medical) on internal networks and other security functions to communicate within and across departments. Nomadic users wanting to "phone home" represent another set of security requirements. These mobile user requirements must be tempered with bandwidth challenges. Additionally, security functions associated with multicast communications add complexity to the required solution set.

This dissertation presents an architecture for network security

management that will allow an organization to provide a consistent security posture for all of its communications, both internal and external. A significant part of this network security management architecture is the ability to **negotiate security** services and mechanisms to protect communications. Security protocols under development are attempting to incorporate security mechanisms in their specifications to protect against attempts to exploit communications across these networks. The security mechanisms that are typically implemented include confidentiality, integrity, authentication, access control, and non-repudiation.

This dissertation also presents a negotiation protocol which provides communicating entities with the ability to **negotiate** the **security** functionality they desire. This is accomplished through the use of a **security association** (SA), which is a relationship between two or **more** entities describing how **security** services will be used to communicate securely. **Security associations** must support multiple **security** services and mechanisms for the Internet Protocol (IP) suite, as well as for other security protocols. Modeling and performance results associated with the proposed **security negotiation** protocol are included in this dissertation.

15/5/2 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2237040 NTIS Accession Number: ADA401378/XAB
Dynamic Parameterization of IPSEC
(Master's thesis)
Agar, C. D.
Naval Postgraduate School, Monterey, CA.
Corp. Source Codes: 019895000; 251450
Dec 2001 334p
Languages: English Document Type: Thesis
Journal Announcement: USGRDR0219
The original document contains color images.
Hard copy only. Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A16/MF A03
Country of Publication: United States
The Internet has become the medium of choice for communications between most Government and Military organizations. Unfortunately the key Internet protocols were not designed to provide security and their security vulnerabilities have become apparent. **IPsec** was developed to provide users with a range of security services, for both confidentiality and integrity, enabling them to securely pass information across networks. Automated security mechanisms are typically designed and/or calibrated to meet an organization's security policy. However, once the mechanism in operation the implemented policy is in a static state, and cannot be adjusted according to dynamic environmental conditions. This means that security mechanisms fail to reflect the policy that is appropriate for the changing contexts. Dynamic parameterization enables security mechanisms to adjust the **level** of **security** service 'on-the-fly' to respond to

changing conditions (i.e., INFOCON, THREATCON). This work includes the extension of the attributes encoded by the KeyNote Trust Management System and modification of the **IPsec** mechanism to incorporate dynamic **parameters** into the **security** service selection mechanism, and the construction of a graphical user interface, for demonstrating 'proof-of-concept' of Dynamic Parameterization of OpenBSD 2.8 **IPsec**.
Descriptors: *Information security; Policies; Automation; Management planning and control; Vulnerability; Theses; Internet; Military organizations; Graphical user interface
Identifiers: Sad(**Security association** database); Sa(**Security association**); Spd(**Security** policy database); NTISDODXA
Section Headings: 62GE (Computers, Control, and Information Theory--General)

****

FULL TEXT NPL

****

File 88:Gale Group Business A.R.T.S. 1976-2006/Mar 14
(c) 2006 The Gale Group
File 369:New Scientist 1994-2006/Aug W4
(c) 2006 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2006/Mar 21
(c) 2006 ProQuest Info&Learning
File 15:ABI/Inform(R) 1971-2006/Mar 21
(c) 2006 ProQuest Info&Learning
File 16:Gale Group PROMT(R) 1990-2006/Mar 21
(c) 2006 The Gale Group
File 9:Business & Industry(R) Jul/1994-2006/Mar 17
(c) 2006 The Gale Group
File 13:BAMP 2006/Mar W2
(c) 2006 The Gale Group
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 610:Business Wire 1999-2006/Mar 21
(c) 2006 Business Wire.
File 647:CMP Computer Fulltext 1988-2006/Apr W2
(c) 2006 CMP Media, LLC
File 98:General Sci Abs 1984-2004/Dec
(c) 2005 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2006/Mar 20
(c)2006 The Gale Group
File 634:San Jose Mercury Jun 1985-2006/Mar 20
(c) 2006 San Jose Mercury News
File 275:Gale Group Computer DB(TM) 1983-2006/Mar 20
(c) 2006 The Gale Group
File 47:Gale Group Magazine DB(TM) 1959-2006/Mar 20

(c) 2006 The Gale group
File 75:TGG Management Contents(R) 86-2006/Mar W2
(c) 2006 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2006/Mar 20
(c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Mar 21
(c) 2006 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2006/Mar W2
(c) 2006 ProQuest
File 613:PR Newswire 1999-2006/Mar 21
(c) 2006 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Dec
(c) 2005 The HW Wilson Co
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2006/Mar 21
(c) 2006 Dialog
File 553:Wilson Bus. Abs. 1982-2006/Mar
(c) 2006 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Mar 20
(c) 2006 The Gale Group
File 674:Computer News Fulltext 1989-2006/Mar W2
(c) 2006 IDG Communications

Set Items Description
S1 190826 VPN OR VIRTUAL()PRIVATE()NETWORK? ?
S2 52288 IPSEC OR (IP OR INTERNET()PROTOCOL)()SECURITY OR IPSECURITY OR IKE OR INTERNET()KEY()EXCHANGE OR ISAKMP
S3 323334 TUNNEL? ? OR SECURE(3N)(CONNECT???? OR LINK? ?) OR SSL OR - SECURE()SOCKET()LAYER
S4 64987 SECURITY(3N)(ASSOCIATION? ? OR PARAMETER? ? OR SETTING? ? - OR CONFIGURATION? ? OR PROPOSAL? ? OR NEGOTIAT????)
S5 195 S4(3N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REA-RRANG??? OR ARRANG???)
S6 688988 SECUR???(3N)(MORE OR MOST OR HIGH??? OR GREATER OR GREATEST OR INCREAS??? OR MAXIMIZ??? OR MAXIMIS??? OR MAXIMIZATION OR MAXIMISATION OR MAXIMUM)
S7 101027 SECUR???(3N)(LESS OR LESSEN OR LESSENED OR LESSENING OR LE-AST OR LOW??? OR DECREAS??? OR MINIMIZ??? OR MINIMIS??? OR MI-NIMIZATION OR MINIMISATION OR MINIMAL OR MINIMUM)
S8 7 S1:S3(S)S5
S9 3 RD (unique items)
S10 17 S5(S)(S6 OR S7)
S11 14 RD (unique items)
S12 12 S11 NOT S9
S13 8 S12 NOT PY=2002:2006
S14 135 S1:S3(S)S4(10N)(S6 OR S7)
S15 107 S1:S3(S)S4(4N)(S6 OR S7)
S16 6614 (S6 OR S7)(3N)(SORT??? OR ORDER??? OR RANK??? OR REORDER??? OR REARRANG??? OR ARRANG???)
S17 2 S16(S)S4(S)S1:S3
S18 26 S16(S)S4
S19 17 RD (unique items)
S20 12 S19 NOT PY=2002:2006

S21 7 S20 NOT (S9 OR S13 OR S17)
S22 180705 SECUR???(3N)(LEVEL? ? OR TIER? ? OR AMOUNT? ? OR STRICT? OR DEGREE?)
S23 160 S22(S)S4(S)S1:S3
S24 59 S23(S)(S6 OR S7)
S25 51 RD (unique items)
S26 28 S25 NOT PY=2002:2006
S27 27 S26 NOT (S9 OR S13 OR S17 OR S21)
? logoff hold
21mar06 16:56:46 User259273 Session D347.17

9/7/2 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06646934 Supplier Number: 55793470 (THIS IS THE FULLTEXT)
VPNware VSU-1100 Sets the Pace.(Hardware Review)(Evaluation)
Fratto, Mike
Network Computing, p46
Sept 20, 1999
TEXT:
VPNet Technologies VPNware System VSU-1100
Network Computing Editor's Choice
Grade: B+

VPNet has focused tremendous energy on making a system that simplifies VPN management, integrates seamlessly into the network and leverages common network services. And it has found much success. Even though the management capabilities are still hobbled by Java in a Netscape Navigator 3.05 browser, there is little to detract from the VPNware System VSU-1100. It provides a straightforward management system that is easy to navigate and intelligently distributes VPN policy configurations to gateways. Nearly every process from initial configuration to CA enrollment is clear-cut and carefully designed.

The VSU-1100 is no slouch when it comes to pushing packets either. Even running 3-DES encryption and MD-5 authentication, the VSU-1100 topped out at 81-MBps throughput. RedCreek's Ravlin 7100 was the only competitor close, at 79 MBps. But, of course, no system is perfect. We occasionally had to refresh the VSU-1100 configuration when making changes and its event logging desperately needs help. VPNet said it is aware of these problems and will address them in version 3 of VPNware. The benefits far outweigh the problems, however-and you'll have to pay a premium for it. The VSU-1100 is priced at $7,000 more than TimeStep's Permit/Gate 7520, but throw in 1,000 clients and its price is on par with Assured Digital's ADI-4500.

Dropping a device into your network without disruption is no mean feat, but the VSU-1100 proved to be up to the task. Like most of the other products that we tested-with the exception of the Assured Digital ADI-4500-the VSU-1100 is able to sit transparently next to a router or act as a router. The flexibility is important because renumbering a subnet is a difficult and time-consuming task; transparent installation helps ease the transition.

Likewise, with the VPN gateway acting as a router you can add subnets without increasing the router ports. Because the VSU-1100 can pass data in the clear, you can much more easily add services where they're needed.

Unfortunately, we found passing data in the clear difficult with the VSU-1100 because we could slice our subnet only based on bitwise boundaries similar to subnetting an IP network. This is needlessly complicated and may require you to reconfigure your hosts to place them into subnet ranges. Like other VPN devices, with the exception of RadGuard's cIPro-VPN, you are better off positioning your management station and servers outside the VPN if possible.

VPNet's model for configuring VPN is relatively risk-free. Within VPNmanager, we grouped together subnets that were to participate in the VPN and assigned each group to a specific VSU. We then created the VPNs by combining groups and setting the encryption policies. Once complete, VPNmanager pushes the configuration out only to the affected VSUs. We also configured multiple VPNs between the same VSU-1100 with differing levels of encryption. Only cIPro-VPN could manage this task.

Support for existing services is well implemented in the VSU-1100. Leveraging a RADIUS server for remote user authentication or syslog for logging is not a problem. Even certifying with a CA was relatively painless. From the VPNmanager suite, we generated a PKCS #10 certificate request and transported it to our Entrust CA by floppy disk. We certified the request and carried the file back to the VPNmanager.

However, we ran into a problem when we tried to import the certificate. When Entrust 4 generates a signed certificate, it doesn't enter in the begin and end certificate lines, a common but optional practice. Therefore, when we tried to import the signed certificate, the VSU-1100 incorrectly perceived it as a PEM (Privacy Enhanced Mail)-encoded file and wouldn't parse the file. We had to enter in the lines manually, and then the certificate was accepted. According to VPNet officials, they will address this issue in the future.

VPNet has enhanced its client support. Configuration files can now be downloaded dynamically when the user connects to the VSU. Client installation is painless, as was the case with all the products we tested. We initially used a configuration file that we exported to a file. We simply started the client and pointed it to the appropriate configuration file.

We next used the dynamic download feature, which requires a user to supply login credentials as well as the VSU certificate name. Once the user is connected, the client is configured. This is an excellent option for traveling users who share a pool of laptops.

VPNware System VSU-1100, $17,995 for hardware only, VPNet Technologies, (888) VPNET-88, (408) 445-6600; fax (408) 445-6611. www.vpnet.com or info@vpnet.com

TimeStep Permit/Gate 7520

Grade: C+

TimeStep's Permit/Gate 7520 sits at the top of the Permit product family, with support for 100-MB networks. If you're familiar with other Permit products, you should feel right at home using this VPN. TimeStep made some modifications to the software on the 7520 and ICSA certification is in progress. That shouldn't deter you; TimeStep is active within the IETF and in the IPSec community that's moving the IPSec standards forward and helping to ensure interoperability. Besides supporting Fast Ethernet, the 7520 supports bridge-emulation mode-it can sit transparently. Like the VSU-1100, it only uses one IP address, unlike the Ravlin 7100 and cIPro-VPN, both of which require two. TimeStep's VPN configuration is fairly straightforward, and in some cases is more granular that VPNet's, but it's also more complex. In terms of performance, the Permit came in last with only 45 MBps. That's still pretty fast throughput, but it's

nowhere near the numbers rung up by either RedCreek's Ravlin 7100 or VPNet's VSU-1100.

Permit gates use configuration files to determine how VPNs are constructed. This is a multistep process. Each gate has a Red Security Policy Table that defines the subnets and hosts on the red (protected) network. The gates are extremely flexible, offering wide support for a number of syntax rules to specify protected addresses. For example, traditional subnetting (similar to VPNet), such as 192.168.201.0/255.255.255.0, wild cards, such as 192.168.201.*, and address ranges, such as 192.168.201.[1-254] all denote the same configuration. We learned early on that we had to be careful building the Red Security Policy table because it acts like a routing table. At one point, we forgot to add an entry allowing management to pass through. As a result, we found ourselves cut off from the rest of the network.

Once all the Red Security Policy tables were built, we selected the devices in our VPN and used the Secure Map Wizard to create the VPN policy definitions to be sent to each gate. The Secure Map is a text file that defines the protected networks in a VPN, the gates they are associated with, and whether they are tunneled or passed in the clear. Because this is a text file, you can edit it by hand, making any modification that's necessary. In a large map, you may want to use the Name parameter to give a descriptive name to an entry, such as "Accounting Department." Unfortunately, any entries you enter into the map by hand, such as the descriptive name, will be erased if you create a new one. Once the map was built, we sent it to all the gates from Permit/Config.

A Security Level Map contains entries specifying what combinations of **IPSec** protocols and cryptographic algorithms are acceptable on the gate. A default Security Level Map contains the most common combinations of groups and are associated with a Security Level Name. This map is a text file that can be edited if custom configurations are required. When a peer gate tries to negotiate an **IPSec tunnel**, the gates only will **negotiate** mutually acceptable **security proposals**.

The **order** of entries in the Security Level Map is important. Two gates will negotiate the first set of mutually acceptable protocols, not the most secure set of protocols. If two gates can negotiate either DES or 3-DES, but DES is listed first, DES will be negotiated. Thus, in cases where you must negotiate DES internationally and 3-DES nationwide, you must edit the Security Level Map to set the proper order.

Both the Secure Map and the Security Level Map are well documented, and the combination of these two files offers an extremely scalable architecture for building common VPNs. For example, two gates in the United States can accept either DES or 3-DES encryption while a gate in France may only support DES. By applying the appropriate Security Level Maps on each gateway, the two gates in the United States will negotiate a VPN using 3-DES while a VPN with France will negotiate DES without having to define individual tunnels on each gate.

The 7520 currently supports only the Entrust PKI (versions 3 and 4), but TimeStep expects to have generic X.509 support by the end of September. The Entrust Support is rock solid, however. The Permit institutes an Entrust client, and we easily certified our 7520 with Entrust online. However, the gates will not work with Entrust 4.0a. We had to upgrade our Entrust PKI to 4.0c. The Permit/Director, TimeStep's policy management system, also leverages Entrust's Directory by pushing group attribute certificates into the directory. The Group attributes define which gates can create a VPN together and offers a better control system than the process of manually creating and editing Secure Map for every gate.

The Permit/Client is extremely configurable and easy to use, though it may appear daunting to novice users and administrators. Fortunately, the client uses the same Security Level Map and Secure Map that the gates use, so no separate configuration files are necessary. After installing the client, we were up and running with a VPN within minutes. TimeStep also provides additional methods for locking down the client besides either user access or no access. Through a user interface file, administrators can lock specific portions of the client from modification.

Permit/Gate 7520, $10,995, TimeStep Corp., (880) 383-8211, (613) 599-3610; fax (613) 599-3617. www.timestep.com or info@timestep.com

RedCreek Communications Ravlin 7100

Grade: C+

RedCreek Ravlin's claim to fame is speedy performance, but while its management has gotten better since the last time we tested it, many of our original complaints still have not been addressed. Configuring the Ravlins and the VPNs between them is a tedious process. We had to touch every configuration option on each Ravlin. The Ravlins support multiple security policies for VPNs; unfortunately, RedCreek supports only X.509 certificates issued by RedCreek. While this is adequate for small shops, managing more than just a handful would take up way too much time. Client support is decent on the desktop.

Although the Explorer-like interface in Ravlin Node Manager (RNM) appears to ease configuration, it's actually pretty time-consuming to configure VPNs. The problem arises because both sides of the VPN need to be configured identically for the VPN to negotiate correctly. We had to select the IKE parameters, the IPSec parameters, the source and destination networks for the VPN, and the shared secret between them. All of this has to be entered into each Ravlin participating in the VPN. Although we had only two Ravlins, we found ourselves constantly flipping between configuration windows to make sure the configurations were installed correctly. Add to this the danger of cutting yourself off from the remote side, which happened more than once, and the GUI management does nothing to ease the configuration burden. Both ADI and VPNet wisely leverage a basic strength of computers-figuring out predictable sequences and applying them. Now try to manage and configure 10 or more Ravlins with RNM and the difficulty grows. That's not to say RNM is all bad, it's just not well suited to large-scale VPNs.

The logging features for the Ravlin 7100 are decent. During initial configuration, VPNs were not becoming established, and we were able to determine why: We had mistakenly mismatched configurations. Logging for remote clients was a little weaker as the messages are fairly cryptic.

We also found that some of the messages are misleading. For example, when we were configuring RADIUS, we added the new network for the RADIUS server but could no longer access the Ravlin because of a profile mismatch. However, the logs only mentioned one side of the problem-we could see that the management station had failed the filter, but not which filter.

The Ravlins support only a single VPN between a pair of Ravlin units. If you want to have multiple security associations between Ravlin units-you might want to have VPNs with valuable data rekeying more often than VPNs with less valuable data-you will need more than one Ravlin at the remote site. But it's affordable: At $17,500 for a Ravlin 7100 and 1,000 clients, it earned our Best Value award.

Ravlin 7100, $7,500, RedCreek Communications, (888) 745-3900, (510) 745-3900; fax (510) 739-0058. www.redcreek.com

Assured Digital ADI-4500

Grade: C

Assured Digital ADI-4500 offers fewer configuration options than any of the other devices we tested and it fared little better in performance than TimeStep's Permit/ Gate 7520. But to its credit, what ADI-4500 does, it tends to do well. Seamless installation and near error-proof configuration and management are the hallmarks of this device. Performance is not. Achieving barely more than 50 MBps throughput, the ADI-4500 was far slower than either VPNet's VSU-1100 or RedCreek's Ravlin 7100. Despite this performance differential, if the ADI-4500 supported features such as transparent installation and configurable subnet participation, it would have been in serious contention with VSU-1100 for the top spot. Unfortunately, ADI assumes that you will install the ADI-4500 as a router and that all the subnets behind the ADI-4500 are to be protected. These are two assumptions that don't fit all instances. For example, a remote office may need a VPN to the main office while still accessing the Internet.

ADI's strength is foolproof VPN construction within ADI Management System (AMS). Once the ADI-4500s are defined, located and authenticated by the AMS, the bulk of the work is done. All that's left is to configure the specific security requirements for each VPN. Within the AMS, ADI devices such as ADI-4500 and ADI-100 clients are placed into administrative domains. This makes up a logical grouping of devices that share a common VPN. Normally devices can't exist in more than one domain, but the ADI-4500 can. We placed our ADI-4500 in the same domain, created a VPN using 3-DES encryption and MD-5 authentication, and we were finished. The AMS updated the ADI-4500s with the new configuration. No stress, no mess. There are additional options unique to the ADI-4500, including setting a default VPN route and forwarding DHCP requests across the VPN.

The ADI-4500 is an all-or-nothing proposition in regard to VPN. Traffic is either tunneled or it isn't. There is no provision for passing traffic in the clear through a ADI-4500 and when we asked ADI representatives about that, they wanted to know why we would ever want to do that. In many cases there's traffic, within an intranet or extranet, that needs to be secured through a VPN and some traffic destined to the Internet should pass in the clear. More important, any services used by any of the ADI-4500s needs to be accessible to all of them. This became a notable problem when we tried to certify our gateways because our Entrust CA was installed on the protected network. We couldn't pass traffic in the clear, so we couldn't certify both devices. We would have had to move our CA. That's certainly not a task you want to undertake in an enterprise setting.

By the same token, we had to install our AMS on the unprotected network because all the ADI-4500s need to communicate with it as well. In some cases, you need to have your management station on the Internet if you want to protect your entire network.

We did certify one ADI-4500 with our Entrust CA. Oddly enough, this is such a new feature that we had to do it on the command line, which will become a feature in the future, though ADI is making it available to installations who require it. Like TimeStep's Permit/Gate 7520, the ADI-4500 has a client that can request Entrust certificates online. With a few commands we were done. Currently, certificate-based IKE VPN configuration is still accomplished on the command line as well.

Client support is very good. The client isn't intimidating from a user perspective. Managing users with AMS is equally straightforward. Before users can begin using the ADI-100 client, the administrator has to extract individual licenses from a set of licenses supplied by ADI.

Here's how the extraction process works: The AMS inserts ID and addressing information for the designated ADI-4500, generates a client

license file, and encrypts it with a password you will supply to the user to unlock the file. Once that is complete, the client disks and ID file are ready for installation. You have the option to configure ADI-100 devices individually, though bulk management is more efficient in large user populations. If you are migrating users from modem-pool remote access, the ADI-4500 can authenticate them against your existing RADIUS server. We added RADIUS support in minutes.

ADI-4500, $9,995, Assured Digital, (888) 234-8767, (978) 486-0555. fax (978) 486-3772. www.assured-digital.com

RadGuard cIPro-VPN

Grade: D

RadGuard's cIPro-VPN held its own, with good management functionality, but we couldn't run our performance tests successfully even after swapping infrastructure hardware and downgrading the cIPro-VPN firmware. We also experienced failures in which management communication was cut off even though we could run encrypted traffic through the VPN. It is also the most expensive device-$51,450 with 1,000 clients, though the cIPro-VPN hardware starts at a low $6,450. That's a tempting price if you want to leverage the Internet for either your intranet or extranet.

During installation with our first version of the software (version 3.46), we ran into IP configuration issues in which we were unable to configure out 192.168 subnet as a class B (see "Supernetting a Class C Address," at right). Technically, 192 is a class "C" address range, but there is no reason for that convention to be enforced. Working with RadGuard technical support, we first had to configure the cIPro-VPN with Class C addressing and then change it to Class B through the management station.

When we downgraded to V3.30-J1 at RadGuard's request to solve some performance issues, we were forced to reconfigure our network to a Class C network.

The cIPro-VPN configuration is very much like a firewall, but it's more complex. We first had to enter the VPN configuration rules in the Policy Table and then added Security Policy entries in another table on each cIPro-VPN. Once that was complete, we were able to send ping traffic through the VPN, but not much else. RadGuard surely will discover and resolve the performance issue before long.

cIPro-VPN, $6,450, RadGuard, (877) RADGUARD, (201) 828-9611; fax (201) 828-9613. www.radguard.com or info@radguard.com

Send your comments on this article to Mike Fratto at mfratto@nwc.com.

Sidebar: Client Interoperability Is Still an Issue

One powerful motivation for IPSec interoperability is that it will enable secure IP communications between disparate peers in a multivendor environment. Great strides have been made with LAN-to-LAN VPN interoperability, though implementation is rather complex and prone to error. Subnet naming, mode selection and keying issues abound, but these bumps in the road are being ironed out within the IETF and the IPSec vendor community.

Client-side interoperability poses additional problems because of the nature of remote access. IPSec peers are identified by their addresses during IKE negotiation and by their protected subnets during IPSec negotiation. However, remote users' IP addresses are indeterminate a priori, and can't be relied upon as ID. In single-vendor remote-access environments, clients are identified by some proprietary mechanism, such as a certificate or a user name/password pair. The client is then assigned an IP address local to the VPN gateway and the VPN is formed.

We used TimeStep's Permit/Client and IRE Safenet/SoftPK for

interoperability testing. We also used TimeStep's Permit/Gate 7520 and VPNet's VSU-1100 as gateways. In both cases, we ran into similar issues with forming host VPNs-getting the subnet and identity naming correct in both the client and the gateway. Although manual configuration will get VPNs up and running, there are obvious issues: It's not scalable and requires some expertise on the end user's part to configure or modify the configuration in the field. Neither option works in the general user population.

A number of drafts in the IEFT IPSec working group use different approaches to configuring remote hosts. One method is to exchange configuration information during Phase 1 of the IKE exchange, commonly called Mode Config. The exchange is initiated in either direction by a two-step handshake. The advantage to Mode Config is that it occurs at the initial stages, though it does complicate the exchange. The other option uses a DHCP security association at the start of the VPN session. While DHCP is well understood and can be extended by the vendor, it also adds a step to VPN construction.

Web Links

"Making IPSec Work for You" (Network Computing, Dec. 1, 1998) www.networkcomputing.com/922/922ws2.html

"cIPro-DMZ: More VPN for Your Dollar" (Network Computing, Nov. 15, 1998) www.networkcomputing.com/921/921sp1.html

"ADI-4500 VPN Switch Is a Mixed Bag" (Network Computing, Oct. 1, 1998) www.networkcomputing.com/918/918sp2.html

"IPSec-Compliant VPN Solutions: Virtualizing Your Network" (Network Computing, Oct. 1, 1998) www.networkcomputing.com/918/918sp2.html

"Virtual Private Networks for Sale" (Network Computing, Aug. 15, 1998) www.networkcomputing.com/915/915colmoskowitz.html

InternetWeek's VPN Source Page www.internetwk.com/VPN/default.html

17/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02083463 63353200
ATM's pivotal role
Sweatt, Richard
Telecommunications v34n10 PP: 63-66 Oct 2000
ISSN: 0040-2494 JRNL CODE: TIE
WORD COUNT: 2104

...TEXT: for security policies. The ATM Security protocol also extends the reach and effectiveness of the **IPSec** protocol, but uses fewer exchanges than **IPSec** to affect the same levels of security in the network, and can exchange indexes with and reuse VCs of the **IPSec** protocol. It also supports a larger set of algorithms and extends the coverage of cipher...

...plain text. ATM security uses electronic code blocks and cipher block chaining to provide the **highest** levels of **security** available. Replay **reordering** and label-based access control insures the most robust security

for remote access, while key...

...and synchronisation allows the security to keep up with the latest innovations in attack methods. **Security** service **negotiation** coupled with **security** nesting and scoping combine to provide the highest level of security interoperability available today.

Security...

27/9/22 (Item 8 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

076185
Axent: Response to firewall RFP
Journal: Network World
Publication Date: July 19, 1999
Word Count: 3134 Line Count: 311
Text:
SynopsisThis document details the recommendations by Axent Technologies, Inc. (hereafter referred to as Axent) for the company Happy Pharmaceuticals, Inc. (hereafter referred to customer) with respect to their security needs as the company grows and expands it's network infrastructure. The company requires space for growth and increasing usage of the Internet. Each individual security component needs to fit into their network structure.Some background on the Raptor FirewallWhat is Raptor Firewall? AXENT's Raptor Firewall is a multi-award winning, network security solution that enforces a network security policy for companies of all sizes connecting to the Internet. Raptor Firewall consists of three integrated components that address the security needs of any company connecting to the Internet and includes an application-level firewall, an integrated **IPSEC** -compliant **virtual private network** server and a Graphical User Interface for management of Raptor Firewalls. The Raptor Firewall is designed to be deployed using standard computing hardware and operating systems available on the market today and currently supports:Windows NT on Intel-based serversSolaris on Sun SparcHP/UX on PA-RISCAXENT introduced the world's first Windows NT-based firewall in early 1996. It has been well received in the market as the most stable, feature-rich and secure NT-based firewall available today. What Problems Does Raptor Firewall Solve? The number one concern for companies connecting to the Internet is security. Security is a broad term to represent several needs that the Raptor Firewall can address. The most common needs include:Basic Network ProtectionAccess ControlApplication ControlVirtual Private NetworkingThe Raptor Firewall is designed to provide multiple levels of protection that combine to provide "airtight" security. This is accomplished by using application-aware security proxies that provide both physical and logical separations of all networks connected to the Raptor Firewall. Physical separation is accomplished by requiring each network to be connected to its own Network Interface Card (NIC) in the Raptor Firewall system; logical separation is accomplished by completely disabling routing of network traffic (layer 3) through the system.This double separation and use of intelligent proxies ensures that the Raptor Firewall will have a bias to "fail-safe" - meaning that no traffic will accidentally pass

through the firewall due to a critical failure in the operating system or firewall software. This is in contrast to packet-filtering firewalls that always route packets and will have a bias to "fail-open", allowing unauthorized traffic through. All Firewalls Do Not Provide the Same Level of SecurityMany reviewers have assumed that all firewalls that pass some level of testing by the International Computer **Security Association** (ICSA) or withstand attacks from popular security scanners provide "enough security" or "the same security". The Raptor Firewall goes beyond the bare **minimum security** that any firewall should provide and takes **security** to a **higher level** to approach "airtight" and hassle-free **security** .The **most** overlooked aspects are system hardening (securing the firewall itself) and detection and prevention of attacks embedded in the application data streams such as buffer overrun, backdoor commands, illegal protocol syntax and other such sophisticated threats to security.Basic Network ProtectionProtecting internal networks against basic and well-known network level attacks is fundamental to any firewall system. The Raptor Firewall provides both IP level and application level logic to ensure such protections. These include protections against attacks like IP fragmentation, source routing, IP Address spoofing, TCP SYN Flood, TCP FIN Scan, Teardrop and other such attacks. Many of these are thwarted by an application- **level security** architecture - the architecture recommended by security experts such as Cheswick and Bellovin ("Firewalls and Internet Security").Application ControlBasic network protection is not enough. Many of the most damaging and sophisticated attacks occur through application data streams, not at the IP level itself. Controlling commands and data passed by applications is also important. The use of intelligent security proxies allows the Raptor Firewall to control individual IP applications such as FTP, SMTP, SQL*NET and so forth to ensure that only legitimate application commands and data are passed from one network to another. An example is the ability of the Raptor Firewall to protect against backdoor SMTP commands and buffer overrun attacks found in FTP, SMTP and HTTP data streams. The Raptor Firewall also validates all HTTP 1.1 commands to ensure that illegal or backdoor attacks are filtered out.Access ControlProtection against well-known network attacks lays the foundation to provide controls over who has access to specific resources within a range of parameters. The Raptor Firewall allows a company to control and monitor users and computer systems using the Internet based on the following parameters defined within individual rules:Source and Destination IP address and/or hostnamesTCP and UDP Applications (HTTP, FTP, SMTP, Telnet, etc)Time of Day/Date RangesUsername and password (strong and weak authentication methods)The controls can be broadened or fine-tuned as needed. Individual users and systems or whole groups of entities can be controlled, depending on the security policy being implemented. Unique to the Raptor Firewall is the use of a consolidated, "best-fit" rule system. The firewall administrator creates the access rules in any order (non-order-dependent) and the Raptor firewall will automatically sort them and interpret their use in the **most secure** fashion. All rules are located in a single graphical window for all proxies and services supported by the firewall. These two features are in contrast to other firewalls that either do not have the rules consolidated into one management interface and/or require the rules to be created in a specific "order-dependent" sequence. The Raptor Firewall "best-fit" access rule method allows the firewall administrator to concentrate on the security policy and not the management of the firewall itself.Virtual Private NetworkingNo firewall, by itself, is able to protect against the most damaging and most difficult to detect attacks - snooping of IP packets and modification of such data. Attackers that are in the

right place at the right time can hijack fully authenticated sessions "protected" by a firewall. The only known protection against such attacks is by encrypting the sessions at the packet layer. The Raptor Firewall provides integrated capability to encrypt IP packets flowing between specific computer systems. **VPN** features integrated with the Raptor Firewall allow a firewall administrator to manage and enforce their security policy for encrypted and non-encrypted network traffic with a single product.Key FeaturesInternational Computer **Security Association** CertificationsThe Raptor Firewall has achieved certifications for the implementation of its security mechanisms, including:ICSA Firewall CertificationICSA **IPSEC VPN** CertificationICSA **VPN** Cryptography CertificationThe firewall certification includes hundreds of automated network attacks that were successfully repelled by the Raptor Firewall. The **VPN** certifications include a rigorous review of how the cryptographic functions were implemented and manual verification that the **VPN** functions work as advertised. The **IPSEC** certification verifies that the Raptor Firewall **VPN** server is completely compliant with all mandatory aspects of the **IPSEC** and **IKE** (**Internet Key Exchange**) **VPN** standards as well as proven to be interoperable with other ICSA certified **IPSEC** compliant **VPN** servers.Third-Generation Application **Level Security** ProxiesIntelligent proxies that control and protect all sessions going through the firewall include support for: HTTP, FTP, SMTP, CIFS (NT File and print sharing), SQL*Net, Telnet, Gopher, NNTP, NTP, DNS and generic pass-through proxies for UDP and TCP-based services. Third-Generation refers to the feature set found in the Raptor Firewall proxies that are beyond those found in most other firewalls that have implemented simple proxies. The key features include protections against well-known application-based attacks, content filtering and blocking, bi-directional user transparency, "best-fit" rule ordering, optional logging, optional fast-mode, various strong and weak user authentication methods, multi-threaded proxies and SMP support.Automatic System HardeningThe Raptor Firewall automatically secures the supporting operating system and environment during its installation and continuously thereafter. This is extremely important for a firewall that is hosted on a standard platform. Many other firewalls do not provide this important feature.After installation, the Raptor Firewall continuously hardens the operating system by monitoring that security mechanisms are always enforced. For example, if the administrator installs or enables a back-up service, the Raptor Firewall will automatically disable the service. If file sharing is enabled, it will be disabled.PerformanceTraditionally, proxy firewalls have been known to be slower than **less - secure** , packet filtering firewalls. With the third-generation proxy architecture of the Raptor Firewall, customers can now have the airtight security of a proxy firewall with the required performance to handle 100 Mbit/sec connections to the Internet. The Raptor Firewall on NT has been independently tested along with other proxy and packet filtering firewalls and has proven to be as fast as any others providing the same **level of security** . The latest numbers from the Datacomm/NSTL benchmark showed a performance rating of 45 Mbit/sec for Raptor Firewall on NT. The high performance is based on using multi-threaded, SMP capable proxies that intelligently cache access rules and automatically perform Network Address Translation (NAT). Similar testing of the Solaris Raptor Firewall produced rates as high as 62.2 Mbit/sec.Objectionable Content Filtering The Raptor Firewall's third-generation security proxies for HTTP, Gopher and NNTP (News) have integrated capabilities to filter the content of the data received by such services. These can be based on a weekly updated subscription list and/or

customer-specific access lists. The Raptor Firewall, if licensed, will automatically download weekly updates of CyberPatrol's rating database for Web and News sites that are considered objectionable.It is also possible for a customer to be very restrictive by creating an "allow" list of sites/URLs, excluding all others. This is sometimes desirable for school systems or companies that require the Internet to be used for work-related activities and/or need confidence that only desirable sites are accessed on the Internet.Strong and Weak Authentication MethodsAuthentication of users is very common, both to track internal use of the Internet and to allow only certain people access to internal resources from the Internet. The Raptor Firewall supports the following methods: NT Domain Authentication(firewall sends username/password to PDC for verification) Gateway (on the firewall) authenticationRadius and TACACS+Bellcore S/KeyAXENT Defender Two-Factor Authentication TokenSecurity Dynamics SecureIDCryptoCard. For interactive services such as FTP, Telnet and HTTP, the third-generation security proxies transparently prompt for authentication, even when users are not aware of the firewall. NT Domain Authentication is very important and not supported by most other firewall products. This allows a company to use existing user databases, maintained on NT Primary Domain Controllers, to control user access through the Raptor Firewall without the need to replicate user databases on the firewall.Intuitive Management InterfaceThe Raptor Firewall can be completely managed, either locally or remotely, through the Raptor Management Console (RMC) under Windows NT and the Raptor Console for Unix (RCU) under Unix. The GUI has the following key features:Remote sessions secured via user authentication and encryption of dataManagement of multiple Raptor Firewalls from a single GUISecurity Proxies and **VPN** connections managed under one GUIAbility to "import" user databases for Gateway Authentication and **VPN** accountsReal-time Monitoring of active sessionsAutomatic alerting via e-mail, SNMP, multimedia and custom program for specific log eventsIntegrated Virtual Private Networking The Raptor Firewall was the first firewall product to integrate **VPN** over three years ago. The **VPN** server is a fundamental part of the firewall that is optionally enabled based on a valid license key. The **VPN** server is used in one of any three modes:Raptor Firewall to Raptor Firewall encryption of IP packetsRaptor Firewall to any **IPSEC** compliant **VPN** server productClient PC (using RaptorMobile) **VPN** to Raptor FirewallRaptor Firewall **VPN** Server is currently one of only a few **VPN** servers that have achieved the rigorous ICSA **IPSEC** and **VPN** Cryptography certifications. The RaptorMobile Client **VPN** product is currently the only product in the market that is ICSA **VPN** Cryptography certified, providing the only completely certified **VPN** solution for secure client-to- server **VPN** .The Raptor Firewall **VPN** Server implements all mandatory aspects of the IETF **IPSEC** standard for encryption of IP packets and the **IKE** Key management protocol. With this, the **VPN** server supports both single DES and 3-key triple DES encryption and MD-5 and SHA-1 message digests. Dynamic key management is supported along with the ability to provide Perfect Forward Secrecy (PFS) using a mechanism to change keys within a session on a periodic basis.A particularly useful feature of the **VPN** server is the optional capability to force any or all **VPN** traffic to flow through the intelligent security proxies. This allows a customer to get detailed logging of **VPN** connections, application **level** controls and **security** protections and additional user authentication methods. Customer RequirementsThe customer has stated some very important points that they require, as follows:The solution must be highly available.The solution must be able to support a single T3 connection to the Internet at any give

time.The internal connection to the firewall systems will be 100Mbit fast Ethernet.The external connection to the firewall systems will be (T3) 45Mbit.The solution should be able to handle more than 3000 possible concurrent sessions, mainly being FTP and HTTP traffic. This should also provide room for growth.The solution should be implemented with NAT (Network Address Translation).All firewall systems should be managed centrally.Logging and reporting of each system should be easily possible.The firewalls should be pro-active in their alerting schemes, so that an administrator is paged when tampering occurs.The customer has provided a simple network diagram detailing their current network, as seen in figure 1. Figure 1.Step 1Initially Axent recommends installing two firewalls at locations Firewall 1 and Firewall 2. These maybe either Unix based firewalls, or NT. As the maximum speed will need to be no more than 45Mbit, both versions of the firewall will handle this capacity. As the Raptor Firewall supports Ethernet, FDDI, Token Ring and ATM, it is an ideal candidate for homogenous environments.These two firewalls will protect the central site from the public. They will be highly available by either:Veritas FirstWatch for Sun Solaris, orMicrosoft Wolfpack (Clustering Service) for NT, orMC Service Guard for HP/UX.These choices depend on what the customer chooses for a platform on which to run their firewalls. Typically this decision is made on the amount of operating system experience that the customer has in-house.The customer can then build rule sets that allow their users to gain access to the Internet for certain services, like HTTP, SQL*Net, FTP, etc. The customer can be assured that all IP traffic is being scanned at the application level, ensuring that only valid, recognized and secure protocol command sets, are being allowed to pass over it.It may also be the case that the company decides in the future that only certain services are available to certain groups or individuals inside the company. The administrator can set up authentication for specific services, forcing certain users to enter a username/password combination before a service becomes available to them.If the first firewall is to go down for any reason, the second firewall, due to the fact that High Availability software is installed and running, will automatically take the traffic over and the users will not notice that something has gone wrong. More information on how the Highly Available solutions can be found on Axent's web site.Step 2The next phase will be to install Raptor Firewalls at locations Firewall 3 and 4 respectively.Even though theses two remote sites are connect to the central site via Frame Relay link, they can also be configured with VPN 's to the firewalls 1 & 2 in case these Frame Relay links are down internally, then they can still communicate with the central site.The users in these remote locations can connect to the Internet via their respective firewalls, with rules sets that have been created by the administrator at his central location.Step 3The administration of these 4 Raptor firewalls will be done from a location in the central site. The administrator will have either a Unix or an NT based Console whereby he can manage all of the firewalls (again either NT or Unix based). All communication between the GUI and each firewall is encrypted and authenticated. He can create rule sets, add users, monitor activity, re-configure, etc. If the internal Frame Relay links go down, he can also manage the firewalls via the encrypted channel over the Internet, to each respective firewall.Step 4Each of the firewalls (1 to 4) will not log their data locally. They will all be configured to pass their logging information to a central server via an encrypted channel. This server will be running Telemate.Net. This is a logging reporting tool, by the company with the same name. It is configured to read in Raptor Firewall log files, and generate Crystal reports based on many

different criteria.Each firewall will be configured to become a pro-active part of the network, meaning that if anything goes wrong, like someone is trying to break into the company network, the firewalls will alert the administrator (group). The alerting mechanisms can be via pager, SMNP trap, client Program, email, etc. If an alert is deemed to be very serious in nature, the firewalls can actually shut themselves down, waiting for an administrator to come and verify what happened.Step 5For the connection of mobile users Axent recommends the Raptor Mobile **VPN** Client. These clients run under Windows 95 & 98 and NT. They allow the user to create a **VPN** **tunnel** between themselves a respective firewall.All data that flows between the clients and the internal network is then encrypted using encryption as specified by the administrator, eg: DES, 3DES, RC2. They may also need to authenticate strongly on the firewalls, using two factor authentication, eg: Axent Defender Token Cards.All communication should be transparent to the user.PricingThree Unlimited NT Axent Raptor Firewalls with **VPN** @$15 000.00 each.One Unlimited NT Axent Raptor Firewalls with **VPN** - Stand By @7 500.00One copy of Telemate.Net reporting Tool @$4 995.00Total Cost of Software: $57 495.00Axent is unable to give prices for both hardware and operating system software. For more informationMore information can be found at the following locations:http://www.axent.com/product/rsbu/firewall/default.htmThis links is the specific page of the Raptor Firewall. It contains a white paper, details the specifics of the firewall, along with certification awards, etc.http://www.telemate.netThis link is to the home site of Telemate.Net, the reporting tool - software company.http://www.veritas.comThis link is to the pages of the highly available software company.http://www.microsoft.comYou can search here for both Enterprise Edition and for WLBS, Windows NT Load Balancing Service.About Axent TechnologiesAXENT Technologies, Inc., is a leading provider of enterprise-wide information security solutions for distributed computing environments. The OmniGuard(r) suite of products enables organizations to centrally manage information security. In addition, OmniGuard provides enhanced data confidentiality, access control, user administration, remote access authentication and intrusion detection across the Internet and intranets for UNIX, Windows(r) 3.x, Windows NT(r), Windows 95, NetWare(r) and mid-range systems. AXENT simplifies the security equation by helping companies address more aspects of enterprise-wide security than any other vendor. Only AXENT turns corporate security policy into reality, making the enterprise network truly secure. Headquartered in Rockville, MD, AXENT offers a broad line of security products used by Fortune 1000 companies and governments worldwide to protect information systems in heterogeneous computing environments. Contact AXENT via e-mail at info@axent.com, or visit AXENT's World Wide Web site at http://www.axent.com

****

WEB RESOURCES

****

ACM: No results
Your search for **+security ipsec vpn "secure connection*" "secure link*" ssl** did not return any results.
Your search for **+"security parameter*" +sort* ipsec vpn ssl** did not return any results.

IP.com: No results
No records matched your search.
Perhaps you should try a less restrictive query.

Search query: security negotiat* sort*

No records matched your search.
Perhaps you should try a less restrictive query.

Search query: security parameter* sort*